REMARKS

Applicant has carefully reviewed and considered the Office Action mailed on September 19, 2006, and the references cited therewith.

Claims 1 and 13 are amended; as a result, claims 1-20 are now pending in this application. Applicant respectfully submits that no new matter is added by this amendment.

Claims 1-3 and 13-18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over WO2001/26322 to Khalil et al. (hereinafter Khalil) in view of U.S. Patent No. 6,948,074 to Borella et al. (hereinafter Borella) in still further view of U.S. Patent Application No. 2001/0016492 to Igarashi et al. (hereinafter Igarashi). Claims 4-7 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Khalil in view of Borella in still further view of Igarashi, and further in view of U.S. Patent Application No. 2002/0062385 to Dowling et al. (hereinafter Dowling). Claims 8-12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Khalil in view of Borella in further view of Igarashi and in still further view of Dowling, and further in view of U.S. Patent No. 6,915,345 to Tummala et al. (hereinafter Tummala). Claims 19 and 20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Khalil in view of Borella in further view of Igarashi, and further in view of U.S. Patent No. 6,785,823 to Abrol et al. (hereinafter Abrol).

Applicant respectfully traverses the rejection of all pending claims, as the features of the claims are neither disclosed nor suggested by the cited references.

In the interests of advancing prosecution, Applicant has amended independent claim 1 to recite (*See, e.g.,* Specification, page. 15, lines 27-30; page 16, lines 1-2; page 16, lines 7-13; FIGURE 5, messages 550 and 560):

> 1. (Currently Amended) A system for a secure key distribution protocol in AAA for Mobile IP, comprising:
>
> an MN that is configured to: generate a Reg-Req message that includes Diffie-Hellman parameters that are used to generate session keys and produce signatures; initiate an authentication session by sending the Reg-Req message; receive a Reg-Reply message that includes session keys that may be used to directly communicate with the AAAH, AAAF, HA, and FA nodes while the MN is in a foreign authority, wherein the session keys are encrypted and wherein the session keys include a first at least one key, a second at least one key, and a third at least one key;
>
> an FA that is configured to: receive the Reg-Req message; ensure that the authentication session is valid; and when valid, sign and send the Reg-Req

message; otherwise, end the authentication session; receive, and authenticate the Reg-Reply message, decrypt at least one key of the session keys; sign, and send the Reg-Reply message to the MN;

an AAAF that is configured to: receive and authenticate the Reg-Req message; generate a first at least one key of the session keys using the Diffie-Hellman algorithm and the Diffie-Hellman parameters; add an identifier relating to the Reg-Req message; sign and send the Reg-Req message; receive, authenticate, sign and send the Reg-Reply message to the FA;

an AAAH that is configured to: receive and authenticate the Reg-Req message; generate a second at least one key of the session keys; sign and send the Reg-Req message including the second at least one key; receive and authenticate the Reg-Reply message; generate a third at least one key of the session keys; encrypt the session keys; sign and send the Reg-Reply message including the third at least one key to the AAAF; and

an HA that is configured to: receive the Reg-Req message including the second at least one key; prepare a Reg-Reply message in response to the Reg-Req message; and send the Reg-Reply message to the AAAH.

In stark contrast, Khalil (per Abstract) is directed to a key exchange for a network architecture. A mobile node that roams over a foreign domain sends a registration request to a home domain using the foreign domain. The identity of the mobile node within the registration request is encrypted. The home domain receives the registration request and decrypts the mobile node identity. The home domain generates a registration reply that includes encryption keys for encrypting information to be transmitted between and among the home domain, the foreign domain, and the mobile node.

The Office Action (page 6, pars. l and o) cites Khalil at page 19, lines 12-23 as teaching "Generate a second at least one key of the session keys" and "Generate a third at least one key of the session keys." The Office Action (page 6, pars. s and t) further cites Khalil, figure 13d, as teaching "Prepare a Reg-Reply message in response to the Reg-Req message" and "Send the Reg-Reply message to the AAAH." However, these portions of Khalil merely discuss a home agent 1010 requesting a distribution center 1024 to generate three encryption keys, and to transmit the three encryption keys to the home agent for distribution to a mobile node 1002 and a foreign agent 1006. The home agent distributes the encryption keys to the foreign agent and the mobile node by generating a registration reply including keys 2 and 3 in unencrypted form and keys 1 and 3 in encrypted form. The home agent then transmits the registration reply to a server for further distribution to the foreign agent and mobile node. Thus, Khalil sends all the keys in one "registration reply" message. A "registration request" is mentioned by Khalil at page 19, lines 3-11, but the is no mention of sending any of the keys 1, 2, or 3 via the "registration request." Thus, Khalil does not teach or suggest "an AAAH" configured to "generate a second at least one key of the session keys; sign and send the Reg-Req message including the second at least one key" and "generate a third at least one key of the session keys; encrypt the session keys; sign and send the Reg-Reply message including the third at least one key to the AAAF" as recited by amended independent claim 1. Furthermore, Khalil does not teach or suggest "an HA that is configured to: receive the Reg-Req message including the second at least one key" as recited by amended independent claim 1.

Borella, directed to a method and system for distributed generation of unique random numbers, does not cure the deficiencies of Khalil in this regard. Moreover, Igarashi, directed to notifying a home agent via a foreign agent, an AAAF, and an AAAH, of location registration information transmitted from a mobile node, also fails to cure the deficiencies of Khalil. Furthermore, no reasonable combination of Khalil, Borella, or Igarashi cures the deficiencies of Khalil with regard to the recited features of amended independent claim 1 discussed above. Therefore, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

The rejection of dependent claims 2-3 should also be withdrawn for at least the same reasons as discussed above with regard to amended independent claim 1, as these claims recite additional features that are also not suggested or disclosed by the cited references.

Independent claim 13 has also been amended to recite, "wherein a first one of the plurality of the session keys is sent by the AAAH via the Reg-Req message to the HA, and wherein a second one of the plurality of the session keys is sent by the AAAH via the Reg-Reply message to the AAAF." For reasons similar to those discussed previously with regard to claim 1, Applicant respectfully submits that the rejection of claim 13 should also be withdrawn.

Similarly, the rejection of dependent claims 14-18, which depend either directly or indirectly from amended independent claim 13, should also be withdrawn for at least the same reasons as discussed above with regard to amended independent claim 13.

With regard to the rejections of dependent claims 4-7 and dependent claims 8-12, Applicant respectfully submits that neither the addition of Dowling nor the further addition of Tummala cure the deficiencies of Khalil, Borella, and Igarashi as discussed previously with regard to amended independent claim 1. Thus, the rejections of dependent claims 4-7 and 8-12 should also be withdrawn.

Regarding the rejection of dependent claims 19 and 20, which depend indirectly from amended independent claim 13, Applicant respectfully submits that the addition of Abrol does not cure the deficiencies of Khalil, Borella, or Igarashi discussed previously with regard to amended independent claim 13. Therefore, the rejection of claims 19 and 20 should also be withdrawn.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (703-652-0853) to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-3521.

Respectfully submitted,

Brake Hughes PLC
Customer Number 53666
703-652-0853

Date December 18, 2006 By Margo Livesay
Margo Livesay, Ph.D.
Reg. No. 41,946

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 18th day of December, 2006.

Laura Bray Laura Bray
Name Signature